# ПОЄДНАННЯ ЗНАННЄВИХ І ЦИФРОВИХ ТЕХНОЛОГІЙ В ЗАБЕЗПЕЧЕННІ ЯКІСНОГО НАВЧАННЯ ФАХІВЦЯ ФІЗИКО-ТЕХНОЛОГІЧНОГО ПРОФІЛЮ

УДК 378:004 DOI: 10.32626/2307-4507.2022-28.62-66

**С. В. Дембіцька[1], М. О. Мястковська[2], Д. Я. Мястковська[3]**

*[1] Вінницький національний технічний університет*

*[2, 3] Кам'янець-Подільський національний університет імені Івана Огієнка*

*e-mail: [1]sofia.dem@i.ua, [2]marinenka1@gmail.com, [3]dashayou9@gmail.com;*

*ORCID: [1]0000-0002-2005-6744, [2]0000-0003-0427-6664, [3]0000-0001-8679-0063*

## ЗАСОБИ АКТИВІЗАЦІЇ НАВЧАЛЬНО-ПІЗНАВАЛЬНОЇ ДІЯЛЬНОСТІ В ПРОЦЕСІ ВИКЛАДАННЯ КУРСУ «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ»

Виклики сьогодення спонукають використовувати різноманітні засоби активізації навчально-пізнавальної діяльності здобувачів вищої освіти в процесі викладання.

З метою активізації навчально-пізнавальної діяльності студентів напряму підготовки 122 Комп'ютерні науки в процесі викладання фахової навчальної дисципліни «Технології захисту інформації» запропоновано: лекційний матеріал розширити сучасними темами, зокрема, темою «Пентест»; завдання лабораторних робіт поглибити актуальними темами, зокрема, «Організація безпеки в комп'ютерній мережі», «Асиметрична криптографія та електронний цифровий підпис на прикладі системи GnuPG»; для реалізації завдань лабораторних робіт використовувати актуальне програмне забезпечення та актуальні версії цього програмне забезпечення.

Завдяки розгляду сучасних тем, реалізації завдань з використанням актуального програмного забезпечення та актуальних версій цього програмного забезпечення, прикладів практичного використання, обґрунтування необхідності вивчення тощо, підходи до активізації навчально-пізнавальної діяльності студентів збагатилися (зокрема, ще й перспективами подальшого розвитку професійного ринку праці та фінансовою мотивацією).

Встановлено, що у студентів викликають велику зацікавленість прикладні теми та завдання, які максимально наближені до практики, до життєвих ситуацій. Оскільки питання, які розглянуті в статті, є завжди актуальними, тому можна продовжувати дослідження з даної теми.

**Ключові слова:** професійна підготовка, активізація навчально-пізнавальної діяльності, комп'ютерні науки, технології захисту інформації, пентест, безпека в комп'ютерній мережі, Wireshark, система GnuPG, Kleopatra.

Наразі пріоритетною метою освітнього середовища є спрямованість на розвиток активності та самостійності особистості в процесі професійної підготовки. Крім того, комп'ютеризація та інтенсивний розвиток всіх галузей науки і виробництва потребують впровадження актуальних освітніх технологій [1]. Сучасні студенти – здобувачі вищої освіти – дуже прагматичні. Виклики сьогодення спонукають використовувати різноманітні засоби активізації навчально-пізнавальної діяльності в процесі викладання.

Проблеми активізації пізнавальної діяльності та оновлення професійної освіти шляхом впровадження інноваційних педагогічних технологій знайшли своє відображення в працях багатьох вчених, зокрема, таких як В. Артамонов, А. Вербицький, В. Вергасов, Р. Гуревич, П. Лузан, О. Пометун та інших. Велику роль у становленні й розвитку активних методів навчання відіграють праці А. Вербицького, В. Лозової, В. Комарова та ін. Проаналізувавши науково-педагогічні публікації з окресленої проблеми ми дійшли висновку, що в процесі професійної підготовки необхідно створити умови, які сприяють успішному оволодінню майбутньою професією, зокрема, за допомогою інноваційних методів і засобів активізації пізнавальної діяльності студентів [1].

Питання захисту інформації є надзвичайно важливими та актуальними сьогодні, оскільки вже давно вийшли на одне з перших місць серед інших завдань, що вирішуються в процесі проектування, створення та використання сучасних інформаційних систем [2]. А ще, особливо, з огляду на війну росії проти нашої держави, і один з її різновидів – кібер-війну!

Ці питання є актуальними і для студентів напряму підготовки 122 Комп'ютерні науки, що спонукало підготувати дану статтю на основі набутого власного педагогічного досвіду, зокрема, при викладанні дисципліни «Технології захисту інформації».

**Мета статті**: на основі аналізу науково-педагогічної літератури та власного досвіду вдосконалити засоби (шляхи) активізації навчально-пізнавальної діяль-

ності студентів напряму підготовки 122 Комп'ютерні науки в процесі викладання курсу «Технології захисту інформації».

В проаналізованих наукових публікаціях наголошено на необхідності впровадження в процес професійної підготовки майбутніх фахівців методів активного навчання. Є різні трактування цього поняття. Наприклад, Т. Вахрушева [3] стверджує, що методи активного навчання – це методи, які передбачають навчання через діяльність. Саме в такому контексті формуються умови свідомого набуття умінь та навичок професійної діяльності, розвитку творчих здібностей та критичного мислення. О. Пометун розмежовує активні й інтерактивні методи навчання та вважає саме активні методи навчання першочерговими для формування професійної компетентності майбутніх фахівців [4].

На нашу думку, будь-яке навчання передбачає певну ступінь активності студента, оскільки за повністю пасивного відношення до освітнього процесу навчання є неможливим. Однак, ступінь цієї активності може бути різною. Незважаючи на різні підходи до трактування змісту методів активного навчання, науковці сходяться в думці, що до них варто віднести такі, які дозволяють студентам в більш короткі терміни і з меншими зусиллями оволодіти знаннями та вміннями за рахунок формування позитивної мотивації до навчально-пізнавальної діяльності. Саме таку самостійну цілеспрямовану навчальну діяльність здобувачів вищої освіти і розглядають як активність особистості [1].

З метою активізації навчально-пізнавальної діяльності студентів напряму підготовки 122 Комп'ютерні науки в процесі викладання фахової навчальної дисципліни «Технології захисту інформації» пропонуємо: лекційний матеріал розширити сучасними темами, зокрема, темою пентесту – тест на проникнення; завдання лабораторних робіт поглибити актуальними темами, зокрема, «Організація безпеки в комп'ютерній мережі», «Асиметрична криптографія та електронний цифровий підпис на прикладі системи GnuPG»; для реалізації завдань лабораторних робіт використовувати актуальне програмне забезпечення та актуальні версії цього програмне забезпечення. Детально розглянемо кожен пункт.

Лекційний матеріал оновлено сучасною темою «Пентест». Питання тестування на проникнення розглядають різні автори, зокрема, Піскозуб А.З. [2], Ric Messier [5] та інші, а особливо пінтестінг досліджують в комерційній сфері [6, 7].

Пентест – різновид захисту комп'ютерних систем. Penetration test (pentest) – симуляція кібератаки на комп'ютерні системи, мобільні застосунки та вебдодатки з метою перевірки захищеності системи. Тест на проникнення допомагає виявити, наскільки та чи інша система є вразливою до хакерських атак [7].

Пентести допомагають оцінити, наскільки легко хакерам отримати доступ до характеристик та даних системи, визначають можливу кількість загроз, а також аналізують негативні наслідки для компанії від реалізованих атак. До того ж, тести на проникнення дозволяють вжити попереджувальних заходів для мінімізації ризиків. Багато компаній використовують пентест як інструмент навчання для своїх спеціалістів з інформаційної безпеки [7].

Відмінності тесту на проникнення (**penetration testing, penetration test, pentest, пентест**) від реальної хакерської атаки полягають в його обмеженнях:

1. Закон. Логічно, що всі дії узгоджуються на підставі договору і дозвільних документів від замовника. Чорні хакери дозволу не питають.
2. Час. Чорні хакери не обмежені у часі, вони можуть роками стежити за «жертвою», виявляючи нові дірки у безпеці (вразливості) в системах, які використовуються, надсилати сотні фішингових листів. У білих, етичних хакерів, є чітко встановлені терміни, які, як правило, обмежені максимум кількома тижнями.
3. Бюджет. Чорні хакери можуть інвестувати значні кошти в наступальні інструменти, так звану кіберзброю (шкідливе програмне забезпечення), включно з покупкою ексклюзивних експлойтів (0-day, вірусів-шкідників, про які ніхто, крім хакерів, не знає). Білі хакери обмежені бюджетом замовників.
4. Глибина проникнення. Ясна річ, що чорні хакери нічим не обмежені, в тому числі й можливістю отримання доступу до всіх систем, які можуть «зламати». Етичні хакери мають обмеження – список систем, до яких можна отримати доступ, обмежується замовником (може і не обмежуватися, що буває рідше) [6].

Різновиди пентестів. З першого погляду може здатись, що тестування на проникнення завжди виконується за єдиним алгоритмом. Насправді, залежно від цілей, існує декілька різновидів пентестів [7]:

- Соціальна інженерія – один з методів отримання персональних даних людини за допомогою телефонної розмови або соцмереж, 80% атак з метою викрадення персональних даних відбуваються саме таким чином.
- Веб-додаток (Web Pentesting) – виявлення вразливості у безпеці веб-додатків та сервісів, встановлених на пристроях клієнта чи серверах.
- Мережева служба (Network Pentesting) – тестування зламу системи, щоб виявити елементи, вразливі до атаки хакерів.
- Клієнтська частина – тестування додатків, встановлених на клієнтському сайті / додатку.
- Віддалене підключення – перевірка vpn чи схожого об'єкта, який може отримати доступ до підключеної системи.
- Бездротові мережі – тест, призначений для бездротових додатків і сервісів, зокрема їх різних компонентів та функцій (маршрутизатори, фільтраційні пакети, шифрування, дешифрування і т. д.).
- SCADA Pentesting – перевірка системи автоматичного збору інформації.

Фази пентесту:

1. Збір інформації про ціль. Охоплює дані, які хакер може знайти у відкритому доступі. Наприклад, імена користувачів, носії, якими вони користуються, відкриті порти, а також відомості про працівників конкретної компанії.
2. Сканування за допомогою програм. Даний етап необхідний для визначення носіїв, які мають відкриті порти, та сервісів, які використовують їх. Також,

хакер завжди перевірить імена користувачів за замовчуванням та паролі знайдених пристроїв.
3. Оцінка виявлених вразливостей. Наступним етапом після збору даних є їх аналіз, який необхідний для розробки подальшого плану атаки.
4. Отримання доступу. Після проведення аналізу, починається найцікавіше: отримання доступу до системи за допомогою виявленої вразливості у сервісах, що знаходяться у мережі жертви. Якщо жодна спроба не завершилась успіхом, тоді хакер береться за співробітників компанії.
5. Звіт. Останнім етапом є створення звіту про всі вразливості, виявлені у системі клієнта. Разом зі звітом надаються дані щодо усунення виявлених вразливостей.

**Режими тестування.** Виходячи з того, який об'єм інформації надається виконавцю про системи (Black Box або White Box), обирається один з наступних режимів тестування [7]:

- White box (відомі всі дані) – виконавець має доступ до більшої кількості інформації, зокрема про структуру мережі, та отримує повний доступ до об'єкта тестування.
- Grey box (дані відомі частково) – комбінація White Box і Black Box підходів. Тобто, налаштування програми нам відомо лише частково.
- Black box (жодних даних) – виконавець знає про діапазон зовнішніх IP-адрес, дані збираються з відкритих джерел (найбільш наближений до дій хакера).

Компанії, які проводять тестування на проникнення, є не лише за кордоном, але і в Україні. Наприклад, минулого року компанія Hacken провела тестування платформ для обміну криптовалют Gate.io та kuna [7].

Ціна тестування на проникнення коливається від 10 до 20 тис. дол. США, в залежності від рівня складності, і тому вартість таких послуг не є непомірною для компаній, у порівнянні з ransomware attack (шифрування даних на комп'ютері жертви за допомогою вірусних програм), де вартість може сягати 50 тис. дол. США (500 дол. США за один пристрій) [7].

Таким чином, пентест допомагає виявити всі вразливості системи. Враховуючи наведені приклади, симуляція атаки є запорукою безпеки компанії. Отже, компанії самі вирішують, чи краще діяти на випередження, або ж долати наслідки. Ринок пентестінга зростає. Згідно з деякими дослідженнями, він складатиме $3,2 млрд. у 2023 році. Що ж впливає на таке активне зростання? По-перше, збільшення кількості користувачів підключених пристроїв по всьому світу. По-друге, зростання кількості бізнес-додатків на базі веб- і хмарних технологій в організаціях. Очікується, що зростаючі потреби у безпеці Інтернету речей (IoT) і тенденція Bring Your Own Device (BYOD) стимулюватимуть зростання ринку тестування на проникнення в найближчі роки [6].

На лабораторному занятті з теми «Організація безпеки в комп'ютерній мережі» студенти: вивчають методи захисту мережі; вчаться здійснювати моніторинг існуючих мережних з'єднань і відкритих портів у комп'ютерній мережі; здобувають навички роботи з програмним засобом аналізу пакетів даних.

Водночас для реалізації завдань лабораторної роботи використовуємо актуальне програмне забезпечення та актуальну версію цього програмного забезпечення: програму-сніфер Wireshark ([8], останню версію). Ми використовуємо сніфер пакетів Wireshark для аналізу змісту повідомлень, відправлених або отриманих різними рівнями стеку протоколів. З технічної точки зору, Wireshark є аналізатором пакетів, який використовує бібліотеку захоплення пакетів комп'ютера PCap (Packet Capture). Wireshark є вільним аналізатором мережевих протоколів, який працює на Windows, Linux/Unix, і Mac-комп'ютерах. Це ідеальний аналізатор пакетів для лабораторних досліджень – він стабільний, має багато прихильників і добре документований [9, 10], а також докладний FAQ [11]. Він має багату функціональність, яка включає в себе можливість аналізувати сотні протоколів, і добре розроблений для користувача інтерфейс. Він працює в комп'ютерах з Ethernet, Token-Ring, FDDI, бездротовими локальними мережами 802.11.

### *Приклади практичних завдань лабораторної роботи*

1. Запустити програму Wireshark та програму-браузер.

2. Ознайомитись з параметрами налаштування захоплення пакетів (Capture Options).

– Запустити захоплення пакетів.
– Зупинити захоплення пакетів.
– Застосувати фільтр «http» до захоплених пакетів.
– Навчитися розкривати / згортати інформацію про вибраний тип протоколу.
– Навчитися зберігати захоплені пакети на диск та відкривати раніше захоплені пакети.
– Визначте кількість та вміст захоплених пакетів протоколу Http.
– Ознайомтеся з текстом запиту Get протоколу Http.
– Відфільтрувати пакети протоколу Http.
– Дослідити перший запит Http Get.
– Дослідити вміст другого запиту Http Get.

3. Перевірити мережу на уразливість (на вибір різні методи, різні варіанти):

– Перевірити мережу на уразливість в «безпечному» режимі, без DoS-атак, у мережі немає сервера баз даних.
– Перевірити мережу на уразливість нових DoS-атак, за допомогою евристичного методу.
– Перевірити мережу на уразливість за допомогою аналізатора скриптів, включивши складну перевірку всіх скриптів.
– Перевірити мережу на уразливість протоколів, для передачі/прийому пошти, використовуючи розширені словники логинів і паролів.
– Перевірити мережу на уразливість, збільшивши час пошуку одного вузла до 5 секунд.
– Перевірити мережу на уразливість, використовуючи весь діапазон портів, з 1 по 65535.
– Перевірити мережу на уразливість у полях запиту Cookie.
– Перевірити мережу на уразливість, збільшивши кількість директорій, що перевіряються, на підбір пароля до 10.

– Перевірити мережу на уразливість, збільшивши кількість потоків для пошуку до 100.
– Перевірити мережу на уразливість, збільшивши час очікування сканування портів.

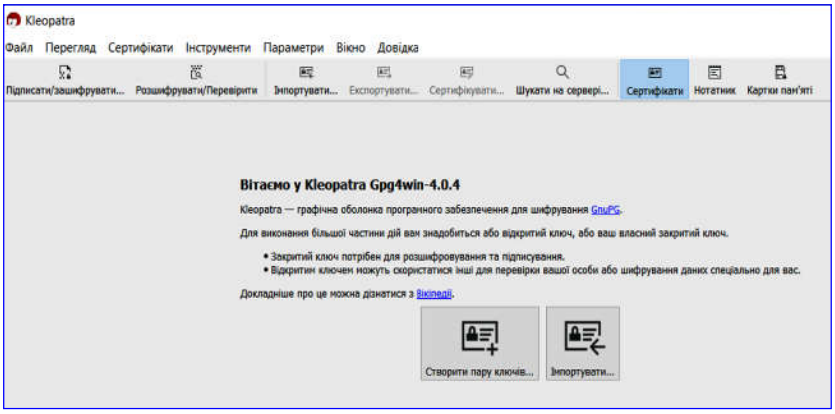


***Рис. 1.*** *Вікно програми Kleopatra*

На лабораторному занятті з теми «Асиметрична криптографія та електронний цифровий підпис на прикладі системи GnuPG» студенти знайомляться з принципами криптографічного захисту інформації з використанням алгоритмів асиметричного шифрування та електронного цифрового підпису, набувають навичок практичного застосування зазначених методів захисту інформації на основі системи GnuPG. Розглядають узагальнений порядок роботи із системою GPG з використанням стандарту OpenPGP.

Виконання криптографічних процесів над інформацією неможливе без наявності ключів шифрування. Для створення пар відкритий/закритий ключ система пропонує використовувати сервер сертифікації Kleopatra (*рис. 1*). Kleopatra – засіб для керування сертифікатами та уніфікований графічний інтерфейс шифрування. Тому для реалізації завдань лабораторної роботи використовуємо актуальне програмне забезпечення та актуальну версію цього програмного забезпечення (версія Gpg4win-4.0.4) [12].

Розробка для лабораторної роботи з теми «Асиметрична криптографія та електронний цифровий підпис на прикладі системи GnuPG» має як опис теоретичного матеріалу, так і детальний опис практичної частини – «Робота з GnuPG та Kleopatra. Версія Gpg4win-4.0.4», що містить пояснення виконання типових завдань: послідовність виконання, скріншоти тощо (*рис. 2*).

### *Приклади практичних завдань лабораторної роботи*

Робота виконується студентами в парі для повноцінного обміну ключами, зашифрованими і підписаними повідомленнями. Кожен зі студентів в парі працює на комп'ютері з встановленою системою GnuPG для Windows. Комп'ютери повинні бути об'єднані в мережу для оперативного обміну файлами. Порядок роботи кожного зі студентів в парі:

1. Створити пару ключів в менеджері ключів Kleopatra.
2. Скопіювати довільний текст в буфер обміну. Зашифрувати вміст буфера обміну за допомогою свого відкритого ключа. Вставити вміст буфера обміну в текстовий редактор, переконатися, що воно зашифровано. Тепер скопіювати в буфер шифротекст, дешифрувати його своїм закритим ключем, знову вставити вміст буфера обміну в текстовий

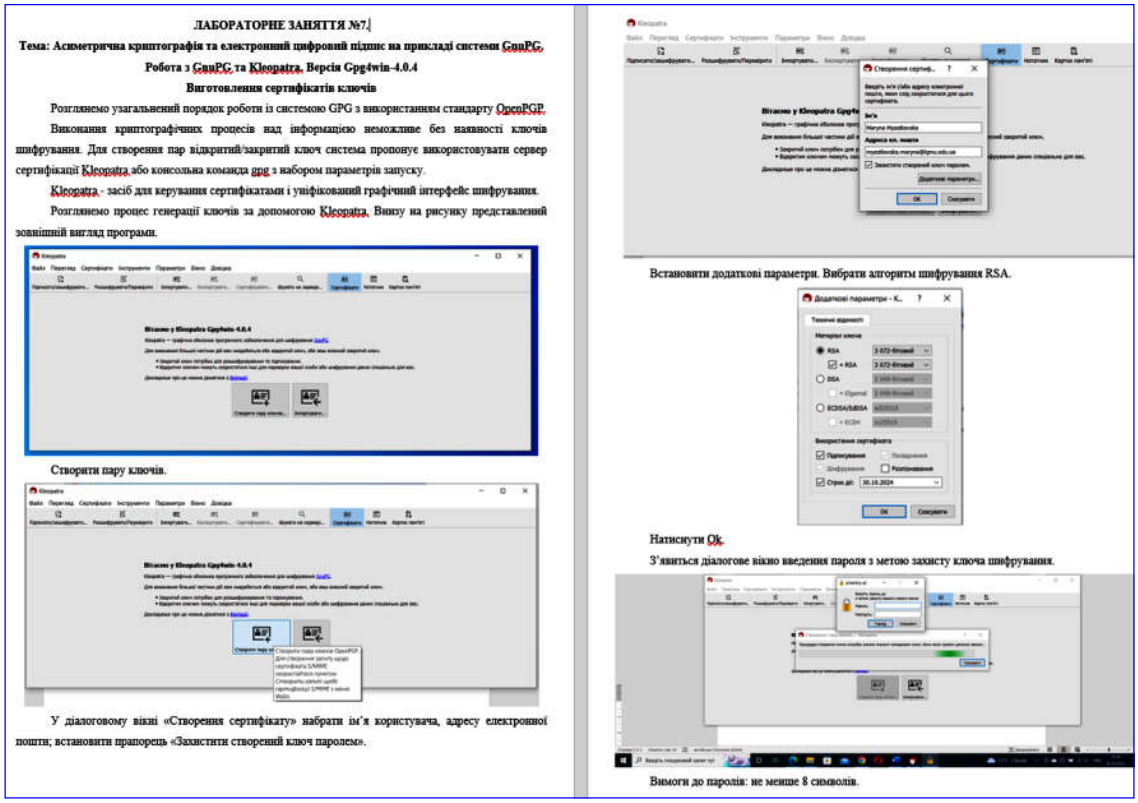


***Рис. 2.*** *Розробка для практичної частини лабораторної роботи (сторінки 1-2)*

редактор, переконатися, що текст був успішно розшифрований.
3. Експортувати сертифікат відкритого ключа зі своєї пари ключів в файл і передати його своєму напарнику.
4. Отримати файл з експортованими ключем від напарника, імпортувати його в менеджер ключів. Встановити для імпортованого ключа повну довіру.
5. Зашифрувати з використанням імпортованого ключа напарника довільний текст на диску. Передати зашифрований текст напарнику.
6. Отримавши зашифрований файл від напарника, дешифрувати його своїм закритим ключем. Переконайтеся, що файл був успішно дешифрований.
7. Використовуючи свій закритий ключ, підписати довільний файл на диску електронним підписом. Передати підписаний документ разом з підписом напарнику.
8. Отримавши від напарника документ з підписом, переконатися, що підпис вірний. Змінити підписаний документ і переконатися, що підпис став невірним. Повернути документ до первісного стану і знову переконатися, що підпис вірний.
9. Скопіювати в тимчасову папку кілька документів. Сформувати для цих документів файл з контрольними сумами. Занести зміни в один або кілька документів і переконатися, що система виявить розбіжності контрольних сум.

Отже, у студентів напряму підготовки 122 Комп'ютерні науки в процесі вивчення курсу «Технології захисту інформації» викликають велику зацікавленість прикладні теми та завдання, які максимально наближені до практики, до життєвих ситуацій.

Завдяки розгляду сучасних тем, реалізації завдань з використанням актуального програмного забезпечення та актуальних версій цього програмного забезпечення, прикладів практичного використання, обґрунтування необхідності вивчення тощо, підходи до активізації навчально-пізнавальної діяльності студентів збагатилися (зокрема, ще й перспективами подальшого розвитку професійного ринку праці та фінансовою мотивацією).

Оскільки питання, які розглянуті в статті, є завжди актуальними, тому можна продовжувати дослідження з даної теми.

**Список використаних джерел:**


1. Дембіцька С.В., Мястковська М.О., Мястковська Д.Я. Сучасні інформаційні технології як засіб активізації навчально-пізнавальної діяльності здобувачів вищої освіти. *Збірник наукових праць Кам'янець-Подільського національного університету імені Івана Огієнка. Серія педагогічна*. Кам'янець-Подільський: Кам'янець-Подільський національний університет імені Івана Огієнка, 2021. Випуск 27: Концепція формування природничонаукової компетентності та світогляду майбутнього фахівця в умовах STEM-освіти. С. 14-17.
2. Піскозуб А.З. Використання тестування на проникнення в комп'ютерні мережі та системи для піднятя їх рівня захищеності. URL: https://science.lpnu.ua/sites/default/files/journal-paper/2017/jun/3676/piskozubaz. pdf
3. Вахрушева Т.Ю. Теоретичні аспекти активних методів навчання. *Педагогіка, психологія та медико-біологічні проблеми фізичного виховання і спорту*. 2008. № 3. С. 46–49.
4. Пометун О.І. Активні й інтерактивні методи навчання: до питання про диференціацію понять. *Шлях освіти*. 2004. № 3. С. 10–15.
5. Ric Messier. Penetration Testing Basics: A Quick-Start Guide to Breaking into Systems / Apress, 2016. 115 p.
6. Пентест: що приховано під білим капюшоном? URL: https://spilno.org/article/pentest-chto-skryvaetsya-pod-belym-kapyushonom.
7. Секрети кібербезпеки: Що таке пентест і навіщо він потрібен компаніям? *European Business Association* (eba.com.ua). URL: https://eba.com.ua/sekrety-kiberbezpeky-shho-take-pentest-i-navishho-vin-potriben-kompaniyam/
8. Офіційний сайт Wireshark. URL: http://www.wireshark.org/
9. Wireshark User's Guide. URL: http://www.wireshark.org/docs/wsug_html_chunked/
10. Manual Pages. URL: http://www.wireshark.org/docs/man-pages/
11. Wireshark Frequently Asked Questions. URL: http://www.wireshark.org/faq.html
12. Сайт проекту GPG. URL: http://www.gpg4win.org/



**Sofiia Dembitska[1], Maryna Miastkovska[2], Dariia Miastkovska[2]**

*[1]Vinnytsia National Technical University*
*[2]Kamianets-Podilskyi National Ivan Ohiienko University*


**MEANS OF ACTIVATING EDUCATIONAL AND COGNITIVE ACTIVITIES IN THE PROCESS OF TEACHING THE COURSE "INFORMATION PROTECTION TECHNOLOGY"**


Today's challenges encourage the use of various means of activating the educational and cognitive activity of students of higher education in the teaching process.

In order to activate the educational and cognitive activity of students in the field of training 122 Computer Science in the process of teaching the professional discipline "Information Protection Technologies", it is proposed to: expand the lecture material with modern topics, in particular, the topic "Pentest"; to deepen the tasks of laboratory work with relevant topics, in particular, "Organization of security in a computer network", "Asymmetric cryptography and electronic digital signature on the example of the GnuPG system"; to use up-to-date software and up-to-date versions of this software for the implementation of laboratory tasks.

Thanks to consideration of modern topics, implementation of tasks using current software and current versions of this software, examples of practical use, substantiation of the need for study, etc., approaches to activating the educational and cognitive activity of students have been enriched (in particular, prospects for the further development of the professional labor market and financial motivation).

It has been established that students are very interested in applied topics and tasks that are as close as possible to practice, to life situations. Since the questions discussed in the article are always relevant, it is possible to continue research on this topic.



**Key words:** professional training, activation of educational and cognitive activities, computer sciences, information protection technologies, pentest, security in the computer network, Wireshark, GnuPG system, Kleopatra.

*Отримано: 11.10.2022*